EXHIBIT 10

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE

ECOLAB Inc., and NALCO COMPANY, LLC d/b/a Nalco Water, an Ecolab Company and/or Nalco Water, Plaintiffs, v. ANTHONY RIDLEY, and CHEMTREAT, INC., Defendants.	Case No. 1:22-cv-00050-TRM-SKL Hon. Travis McDonough Magistrate Judge Susan K. Lee

EXPERT REPORT OF JAMES D. VAUGHN

TABLE OF CONTENTS

I. Credentials and Background

My name is James D. Vaughn. I am a Managing Director of iDiscovery Solutions (iDS) and a court-recognized expert who has given testimony in more than 80 cases involving digital forensic methodologies, including the identification, collection, analysis, and production of electronically stored information. I have also trained hundreds of law enforcement officers, attorneys, and other examiners on digital forensics and high-technology-related issues involving best practices and methodologies. I previously served as a part-time instructor and course developer with the California Department of Justice, where I co-developed and taught digital forensics courses. I am a retired law enforcement officer; I spent the last several years of my law enforcement career conducting digital forensic investigations.

My credentials include professional certifications related to digital forensics. I am an EnCase Certified Examiner (EnCE),[1] as well as a GIAC Certified Forensics Examiner (GCFE).[2] To obtain these certifications, I attended formalized digital forensics training, took written tests, and have performed practical examinations, all of which are designed to measure proficiency. I am also required to renew these certifications by submitting continuing professional education and other formal training credits every three years. To demonstrate my expertise, I have voluntarily maintained active digital forensic certifications for more than 20 consecutive years. Conservatively speaking, I have more than 1,800 hours of formal training in computer, digital media, and mobile device forensics.

[1] The EnCase Certified Examiner (EnCE) program certifies both public and private sector professionals in the use of Opentext EnCase Forensic. EnCE certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase software during complex computer examinations.

[2] The GIAC Certified Forensic Examiner (GCFE) certification validates a practitioner's knowledge of computer forensic analysis, with an emphasis on core skills required to collect and analyze data from Windows computer systems.

I have significant experience performing forensic investigations of computers, mobile devices, storage media, and other devices in lawsuits alleging the misappropriation of trade secrets, confidential information, and intellectual property. I have served as an expert witness and have worked with clients on both the plaintiff and defense side of such disputes, as well as served as a third-party neutral on several occasions. Exhibit A, which is my curriculum vitae, further describes my qualifications and experience, including publications I have authored in the last 10 years, and depositions or trials for which I have provided live testimony for at least the last 4 years.

iDS is compensated for my services in this matter at the rate of $600.00 per hour, plus the cost of other iDS employees performing tasks on this project. That compensation does not affect my opinions in this matter. When I use the word "I" throughout this report, it is intended to represent tasks performed by myself or other iDS team members working under my direction and supervision.

This expert report is provided based on the information presently available to me. I understand that discovery in this matter is ongoing. To the extent additional information or documents are produced in this matter that may bear on my conclusions, I reserve the right to supplement this expert report appropriately.

II. Facts and Assumptions Provided by Counsel

I have been provided copies of all documents produced by each of the parties to this litigation, including any forensic images that have been produced by the parties as of the date of this report, as well as copies of interrogatory responses provided by all parties, and various public court filings by the parties. In the course of preparing this report, including forming the opinions

set forth below, I relied upon the facts set out in the materials cited herein.[3] A complete list of the materials I relied upon for purposes of this report is attached as Exhibit B.

I also relied on certain assumptions provided by counsel for ChemTreat, Inc. ("ChemTreat"). These assumptions, in part, inform the conclusions I reach in this report. The assumptions provided by counsel for ChemTreat upon which I relied in preparing this report are as follows:

- The personal email address for Anthony Ridley ("Mr. Ridley") is aridley75@hotmail.com.
- The file names identified in Search No. 1 are the file names Ecolab[4] identified in its original complaint as file names corresponding to Nalco/Ecolab ("Ecolab") documents Mr. Ridley allegedly misappropriated while employed by Ecolab. Ecolab's March 3, 2022 Complaint, ¶¶ 39, 53, 93 (Doc. 1).
- The file names identified in Search No. 6 are file names corresponding to the file names on the CrowdStrike log in which the phrase "Nalco Water Files" appears in the file path.
- The file name identified in Search Nos. 4 and 5 is a file name of an Ecolab document attached to an email sent from Mr. Ridley's personal email address to his ChemTreat email address.
- The email addresses identified in Search No. 3 are personal or non-ChemTreat email addresses known or alleged to belong to Mr. Ridley.

[3] My opinions do not rely on any party's or witness's characterization of the facts set out in any document or discovery response.

[4] References to "Ecolab" in this report refer to Plaintiffs Ecolab Inc. and Nalco Company, LLC.

- The custodians whose data was provided to me, either during my initial investigation in 2022 or my further investigation in 2023, include individuals in Mr. Ridley's line of authority (including his immediate supervisor, the supervisor to Mr. Ridley's immediate supervisor, and the executive at the head of ChemTreat's North American field sales organization) as well as Mr. Ridley's predecessor, and a number of ChemTreat employees who may have interacted with Mr. Ridley.
- The Lexar USB I examined was issued to Mr. Ridley by ChemTreat and returned by Mr. Ridley to ChemTreat upon his termination.
- David Ellis retired from ChemTreat on December 10, 2021.

III. My Early 2022 Investigation Into Ecolab's Allegations of Misappropriation

I was retained by ChemTreat to investigate allegations made by Ecolab in a February 9, 2022 letter that Mr. Ridley had misappropriated Ecolab's documents and placed them on or distributed them through ChemTreat's systems.[5] I directed the search of potentially relevant ChemTreat repositories and documents in the possession of certain ChemTreat custodians to assess the accuracy of certain allegations made by Ecolab in the February 9, 2022 letter and in a legal complaint filed on March 3, 2022. I found no evidence that Mr. Ridley stored Ecolab's confidential information or documents on ChemTreat's Systems[6] or that he had distributed Ecolab's confidential information or documents to other ChemTreat employees using

[5] February 9, 2022 Ltr. from D. Walton to V. Mirmira (Doc. 42-2) (the "February 9, 2022 Letter").

[6] When I refer to "ChemTreat's Systems" in this report, I am referring to systems managed by ChemTreat that a user could utilize to distribute data, information, or documents, including cloud-based platforms such as OneDrive, network shared folders, and email. ChemTreat's Systems, as used in this report, does not refer to stand-alone devices such as individual laptops.

ChemTreat's Systems. In fact, the investigation revealed just one Ecolab document—a bid document from 2015.[7]

This Section describes the investigation that I conducted in February, March, and April of 2022. Section III.A discusses the sources of electronically stored information I collected and searched. Section III.B describes the searches I conducted. Section III.C describes the results of those searches. Section III.D discusses a search of ChemTreat network or shared folders I directed. Section III.E describes the conclusions I reached as a result of my early 2022 investigation.

A. Key Sources of Electronically Stored Information

My investigation in early 2022 focused on various ChemTreat data repositories that Mr. Ridley could have used to store or distribute information electronically. These sources included: (1) a Microsoft cloud-based document storage platform named OneDrive; (2) a ChemTreat-issued email account that stores emails sent or received by Mr. Ridley; and (3) information regarding Mr. Ridley's activities derived from an enterprise level data protection software program named CrowdStrike, which I describe in further detail below.

Below, I discuss the various data files, information, documents, and devices I searched or analyzed as part of my forensic investigation and any results arising from my review of those data files, information, and documents. My investigation in early 2022 focused on two primary categories: (1) a search of locations Mr. Ridley may have stored documents or from which Mr. Ridley may have distributed documents (such as his email and a Microsoft cloud-based storage platform named OneDrive); and (2) a search of locations that could contain documents potentially

[7] CHEMR-000001631; CHEMR-000001632. I understand Ecolab has stated in this litigation that this document is "not a trade secret individually." Ecolab's January 27, 2023 Supplemental Responses & Objections to ChemTreat's Interrogatories, at page 4.

distributed by Mr. Ridley (such as the emails and OneDrive accounts of other custodians, or ChemTreat's shared network folders).

Based on more than 20 years of experience as a forensic investigator, this investigation was a reasonable search of these locations and would allow me to determine what, if anything, Mr. Ridley had distributed within ChemTreat's Systems or to others with whom I understand he interacted at ChemTreat using ChemTreat's Systems.

1. Mr. Ridley's Repositories

I received from ChemTreat: (1) emails contained in the ChemTreat Microsoft (O365) email system for Anthony Ridley for the period May 1, 2021 to March 16, 2022 (including emails that may have been deleted on or after February 9, 2022, when Ecolab alerted ChemTreat to Mr. Ridley's alleged misappropriation); (2) all OneDrive documents uploaded by or accessible to Mr. Ridley during his employment by ChemTreat (including OneDrive documents Mr. Ridley may have deleted on or after February 9, 2022); (3) the first laptop issued to Mr. Ridley by ChemTreat; (4) excerpts of a CrowdStrike log showing relevant files accessed (opened) from USB devices connected to Mr. Ridley's first ChemTreat-issued laptop before it was reformatted and redeployed; (5) the second laptop issued to Mr. Ridley by ChemTreat; and (6) a USB device returned to ChemTreat by Mr. Ridley upon his termination.

Below, I describe the analysis and search of each of these repositories and devices that I conducted.

a. Mr. Ridley's Emails

As noted above, I collected and searched emails contained in the O365 ChemTreat email system for Anthony Ridley for the period May 1, 2021, to March 16, 2022.[8] The specific searches

[8] There were no emails to Mr. Ridley's ChemTreat email address prior to July 8, 2021, which appears to be the date Mr. Ridley's ChemTreat email address was activated. As noted below, July

I conducted are detailed below. My investigation revealed a single Ecolab document,[9] which is discussed in further detail below.

b. Mr. Ridley's OneDrive Documents

As noted above, I also collected all OneDrive documents uploaded by or accessible to Mr. Ridley. OneDrive is a cloud-based document storage system offered by Microsoft that is used by many businesses, including ChemTreat. OneDrive allows users to share documents with one another using the cloud. However, not all documents within OneDrive are viewable by everyone at ChemTreat. Instead, documents are segmented in specific folders, and the "owner" of a given folder is the only one who has access to the documents in that folder, unless they "share" the folder with another individual at ChemTreat, or unless they have Administrator credentials. This is a standard security configuration that I have seen at dozens of other organizations I have consulted with over the years.

I conducted a search of Mr. Ridley's OneDrive documents. The details of that search are discussed below. The search did not reveal any documents that appeared to contain Ecolab's confidential information. Instead, many of the documents returned as a result of my investigation of Mr. Ridley's OneDrive were clearly ChemTreat documents, and the remainder were either Mr. Ridley's personal documents or documents that did not bear indicia that they belonged to Ecolab. The complete results of this search are described in further detail below.

c. Mr. Ridley's First ChemTreat-Issued Laptop

I received a laptop that had been issued by ChemTreat to Mr. Ridley near the beginning of his employment and shipped back to ChemTreat for purposes of preservation and analysis. I

13, 2021 is the first date on which Mr. Ridley sent emails from his ChemTreat email account. *E.g.*, Ex. C, July 13, 2021 email from A. Ridley to S. Freed.

[9] CHEMR-000001631; CHEMR-000001632.

conducted a forensic analysis of this laptop to determine the extent to which data, documents, and other digital forensics and artifacts could be retrieved from the laptop.

According to the discovery materials provided to me, this laptop was received by ChemTreat from Mr. Ridley on or about March 2, 2022 and was thereafter inadvertently placed with laptops designated for reformatting and redeployment by ChemTreat's IT department.[10] Based on the presence of a second user's profile on the laptop, I determined that the laptop had been redeployed and used by another ChemTreat employee before it was delivered to me. I forensically imaged the laptop's hard drive, but determined that the profile for Mr. Ridley, along with any documents and forensic artifacts associated to that profile, had been removed from the computer during the reformatting process.

d. CrowdStrike Log

In my investigation, I determined that, although the data from Mr. Ridley's first ChemTreat-issued laptop had been removed from it during the reformatting process, other data regarding Mr. Ridley's use of his ChemTreat-issued laptop remained available. Specifically, I reviewed excerpts of a log from a data protection program implemented by ChemTreat called CrowdStrike.[11]

CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting data.[12] Based on my experience, the CrowdStrike platform is a powerful tool that businesses can use to monitor the infiltration of data to business systems, or the exfiltration of data to external USB devices. CrowdStrike maintains a log of all external USBs plugged into a

[10] ChemTreat's July 22, 2022 Responses & Objections to Ecolab's Interrogatories, at pages 13-14.

[11] For purposes of my later investigation, I reviewed a complete copy of the CrowdStrike log. CHEMR-000002195. *See infra*, Sections IV.B and IV.F.

[12] CrowdStrike Home Page, *available at* https://www.crowdstrike.com/.

particular ChemTreat laptop. CrowdStrike also maintains a log of all file names that were accessed by a particular ChemTreat laptop from an externally connected USB device.

I reviewed excerpts from the CrowdStrike log for Mr. Ridley's first ChemTreat-issued laptop that reflected interactions that laptop had with any files in a "Nalco Water Files" folder path.[13] The information I reviewed showed external files were accessed from two USB devices that had been connected to Mr. Ridley's laptop, and reflected log entries for documents that were accessed from those external USB devices from folders whose file path contained the phrase "Nalco Water Files." The data I received showed certain activity that occurred on August 17, 2021; August 20, 2021; and January 28, 2022. The CrowdStrike log excerpts I reviewed is attached as Exhibit D.

The file paths and file names associated with each of these files are listed below:

a. <value><text>\Device\HarddiskVolume5\Nalco Water Files\Account Mangement Examples\~$LCO Master Proposal.dotm</text></value>

b. <value><text>\Device\HarddiskVolume5\Nalco Water Files\Account Mangement Examples\~$mote Service Plan-2020 v1.docx</text></value>

c. <value><text>\Device\HarddiskVolume5\Nalco Water Files\Quint McCreary Files\Magotteaux\PSR\~$gotteaux PSR 2019 05 10.doc</text></value>

d. <value><text>\Device\HarddiskVolume5\Nalco Water Files\Quint McCreary Files\Frito Lay\PSR\~$Nalco Report PepsiCo Service Water Fayetteville Septemeber 2018.xlsx</text></value>

[13] Upon receipt of the complete CrowdStrike report as part of my subsequent investigation in 2023, *see infra*, Section IV.F, I confirmed that the excerpts I received as part of my early 2022 investigation reflected all entries for files contained in a "Nalco Water Files" folder path.

e. <value><text>\Device\HarddiskVolume5\Nalco Water Files\Customers Files - Nalco Water\Volkswagon\Volkswagen service reports\Volkswagen - Media Center\Volkswagen Media PSR 2014\~$lkswagen - Media Center - Chilled Water System 06.11.2014.docx</text></value>

f. <value><text>\Device\HarddiskVolume6\Nalco Water Files\service report notes\~$rvice report technical notes - ver.3.docx</text></value>

g. <value><text>\Device\HarddiskVolume6\Nalco Water Files\service report notes\~$rvice report technical notes.doc</text></value>

The first five documents listed above appear to have been accessed from a USB device that CrowdStrike identified as "HarddiskVolume5." The last two documents listed above appear to have been accessed from another USB device that CrowdStrike identified as "HarddiskVolume6."

The fact that these file names appear in the CrowdStrike log does not mean that they were distributed within ChemTreat's Systems, or even that they were permanently or temporarily saved to Mr. Ridley's ChemTreat-issued laptop. Instead, when a file is accessed from an external storage device, an automatic temporary file is created, which is designated with the "~$" symbols that precede these file names. By design, the operating system deletes the temporary file when the user closes the file. To the extent the temporary file does not get automatically deleted, what remains on the laptop is not the actual file itself and therefore does not contain the content of the document; rather, the artifact that remains is merely a pointer to the actual document.

I searched the file names associated with these documents across all custodians' emails, attachments, and OneDrive folders as part of Search No. 6 below. That search showed that none of these files exist within the emails, attachments, or OneDrive folders for those custodians.

As discussed above, typically, CrowdStrike logs provide information about what files were accessed from external USB device(s) that have been connected to a particular laptop, as well as the date of access, file names, and extensions for those files. This, in combination with the OneDrive documents and emails on ChemTreat's Systems, replicates much of the relevant information that could have been derived from Mr. Ridley's first ChemTreat-issued laptop before it was reformatted. Information that may have been lost due to the reformatting of the laptop prior to redeployment would tend to show Mr. Ridley's personal interactions with any USB documents and the opening of documents on the laptop, as opposed to the dissemination of documents to other ChemTreat employees. For example, the lost data might have included what documents were saved to the desktop of the laptop, but data reflecting any distribution by Mr. Ridley of documents using the laptop would remain preserved through other information that would not be affected by the subsequent reformatting of the laptop, such as email data, or the presence of those files in the OneDrive account of Mr. Ridley or another custodian. Although my investigation was targeted to identify any such sharing, I found no evidence to show that any such sharing had occurred.

Thus, as it pertains to interactions between Mr. Ridley's first ChemTreat-issued laptop and external USB devices containing documents with the phrase "Nalco Water Files" in the file path, the CrowdStrike log contains almost all the relevant data that I would have procured had I been able to forensically image and analyze Mr. Ridley's ChemTreat-issued laptop prior to reformatting. That is, much of the information needed to determine insertion of a USB device, and access of these apparently Nalco-related documents from a USB device, is available through the CrowdStrike logs. Generally speaking, the only information regarding Mr. Ridley's actions that could have been derived from a forensic image of Mr. Ridley's first ChemTreat-issued laptop (and that is not retained in the CrowdStrike log) are artifacts such as evidence of documents that

might have been saved to or modified locally on the laptop hard drive, and (although potentially duplicative of the CrowdStrike log) evidence of documents being saved to the laptop from a connected USB.

As discussed in detail below, *infra*, Section IV.F, I later conducted validation testing to confirm the reliability of the CrowdStrike log, including specifically CrowdStrike's accuracy in logging (1) the serial number of external USB devices connected to a laptop, as well as (2) the file paths of documents accessed from such external USB devices when the log is run after the subject laptop has been reformatted, as it was with Mr. Ridley's first ChemTreat-issued laptop.

e. Mr. Ridley's Second ChemTreat-Issued Laptop

When Mr. Ridley's original ChemTreat-issued laptop was collected from him, ChemTreat issued a second laptop to Mr. Ridley that he could use for work purposes.[14] Upon Mr. Ridley's termination from ChemTreat, ChemTreat IT personnel collected that second laptop from Mr. Ridley for purposes of preservation.[15] That laptop was then sent to me for analysis. I forensically imaged and conducted a forensic analysis of this laptop to assess whether it contained any Ecolab confidential information.

Upon examination of this second laptop, I did not find any evidence of copying or exfiltration of data from the laptop to any other source. Additionally, I was able to identify three USB devices that had been accessed from the second laptop. Two of these USB devices appeared to be devices used by ChemTreat's IT personnel to set up the laptop, as indicated by the username associated with these USBs: "wqadmin." The third USB device was a Lexar USB Flash Drive

[14] ChemTreat's July 22, 2022 Responses & Objections to Ecolab's Interrogatories, at page 26.
[15] ChemTreat's July 22, 2022 Responses & Objections to Ecolab's Interrogatories, at page 26.

bearing serial number 56261F6B34AF1760, that had been connected to the second laptop on just one occasion, March 18, 2022. I discuss the Lexar USB in more detail below.

Based on the interaction with the Lexar USB Flash Drive, I inspected the file access history on the second laptop to determine which files were accessed on March 18, 2022, the date that the Lexar USB Flash Drive was connected to the second laptop. I determined that the only files accessed on that date (less than five documents total) were Mr. Ridley's personal documents based on their file names, including a Marriage Certificate.

I then conducted a search for potentially relevant file names across all "user files" on the second laptop. Specifically, I searched for the file names identified in Search Nos. 1, 4, and 6, described below. The search for these file names returned no hits, meaning that no user files on the second laptop have file names matching the file names searched for.

I also conducted a key word search across all user files on the second laptop. Specifically, I searched for "Nalco" or "Ecolab." After searching for these two key words across the user files on the second laptop, I received 2 results. I reviewed each of the results and determined that neither of the resulting documents bear any indicia that they are Ecolab's documents that may contain Ecolab confidential information. One document was a personal resume of Mr. Ridley, and one document contained personal login credentials.

f. Lexar USB Device – Returned by Mr. Ridley to ChemTreat

When Mr. Ridley was terminated, he returned a USB device to ChemTreat that had been issued to him by ChemTreat. I forensically analyzed this device to assess whether it contained any Ecolab confidential information. The USB device was a Lexar USB Flash Drive, Serial Number: 56261F6B34AF1760, which is the same Lexar USB discussed immediately above.

I analyzed the device and determined that October 26, 2021 was the earliest date that any of the files located on the device had been loaded to it, which I understand is several months after Mr. Ridley departed Ecolab.[16]

I then conducted a search for potentially relevant file names across all files on the USB device. Specifically, I searched for the file names identified in Search Nos. 1, 4, and 6, described below. I also conducted a keyword search for "Nalco" or "Ecolab" across all files contained on the Lexar USB device. These searches resulted in no hits, indicating that there are no documents belonging to Ecolab on this USB device.

2. Emails and OneDrive Documents of Potentially Relevant Custodians

In addition to the repositories and devices associated to Mr. Ridley identified above, I also searched the emails[17] and OneDrive documents of various other custodians with whom Mr. Ridley may have interacted. Specifically, I received from ChemTreat all emails for the period May 1, 2021, to March 16, 2022 that were contained in the O365 ChemTreat email system of the following custodians:[18] Mr. Ridley's immediate supervisor (Clay Cissell), Mr. Cissell's supervisor (Steven Leavell), Mr. Ridley's predecessor (David Ellis), the executive at the head of ChemTreat's North American sales organization (John Alcorn), and a number of ChemTreat employees who may have interacted with Mr. Ridley (Albert DeNunzio, Larry Harmon, Matthew Hofer, Michael (Todd) Kraft, David Pearson, James (Jim) Shealy, George Sloan, and John Spalding). This search included available deleted files from the emails or OneDrive folders of these custodians.

---

[16] Ecolab's June 10, 2022 Second Amended Complaint, ¶ 108 (Doc. 42).

[17] References to "emails" herein refer to emails and their attachments, which are included in the data I received.

[18] I selected the beginning date of this temporal period because Ecolab alleged that Mr. Ridley's exfiltration of data began on May 22, 2021. Ecolab's March 3, 2022 Complaint, ¶ 39 (Doc. 1). The end date of this temporal period was the date these emails were collected from ChemTreat's O365 environment.

I also received all OneDrive documents accessible to or uploaded by the same custodians for whom I received emails, except for David Ellis.[19]

B. Searches Conducted

After receiving the emails and OneDrive data identified above, I loaded the data to Nuix, a forensic industry standard database that iDS uses for processing, searching, and reviewing forensic data. Once processed, I conducted the following searches across these documents:

1. **Search No. 1**:

   i. Repositories: OneDrive documents and emails identified above.

   ii. Custodians: All custodians identified above.

   iii. Search Terms:[20]

      1. 2021 partnership and market overview - simmons foods.pptx
      2. 2021 partnership and market overview.pptx
      3. fb na sales 2021 exprice review for customers.pptx
      4. notes for Maytag 2006 contract.doc
      5. esisting inventory quote.doc
      6. e intensive cleaning procedure covid 19 goggles.docx
      7. monthly tracking report

[19] The OneDrive documents accessible to or uploaded by Mr. Ellis were no longer available at the time of my initial investigation because I am informed Mr. Ellis retired from ChemTreat on December 10, 2021, two months before Ecolab's February 9, 2022 Letter raised the allegations that I investigated. *See supra*, Section II. For the same reason, Mr. Ellis's emails were available dating back to April 29, 2021, which predates Mr. Ridley's earliest alleged downloading activity. Ecolab's March 3, 2022 Complaint, ¶ 39 (Doc. 1).

[20] These search terms are derived from paragraphs 39, 53, and 93 of Ecolab's original complaint, which was the operative complaint at the time of my investigation in early 2022. Ecolab's March 3, 2022 Complaint, ¶¶ 39, 53, 93 (Doc. 1).

2. **Search No. 2**:

    i. Repositories: OneDrive documents received.

    i. Custodians: Anthony Ridley

    ii. Search Terms: ("Nalco" or "Ecolab")

3. **Search No. 3**:

    ii. Repositories: OneDrive documents and emails received.

    iii. Custodians: All custodians identified above.

    iv. Search Terms:

        1. "aridley75@hotmail.com"

        2. "aridley75@live.com"

        3. "aridley@ecolab.com"

4. **Search No. 4**:

    i. Repositories: All emails received.

    i. Custodians: All custodians identified above.

    ii. Search Terms: "AEDC proposal for purchasing – HVAC Cooling Towers – October 2015.doc"

5. **Search No. 5**:

    i. Repositories: All OneDrive documents.

    ii. Custodians: All custodians identified above.

    iii. Search Terms: "AEDC proposal for purchasing – HVAC Cooling Towers – October 2015.doc"

6. **Search No. 6**:

    i. Repositories: All OneDrive documents and emails received.

ii. Custodians: All custodians identified above.

iii. Search Terms:

1. ~$rvice report technical notes - ver.3.docx
2. ~$rvice report technical notes.doc
3. ~$gotteaux PSR 2019 05 10.doc
4. ~$Nalco Report PepsiCo Service Water Fayetteville Septemeber 2018.xlsx
5. ~$lkswagen - Media Center - Chilled Water System 06.11.2014.docx
6. ~$LCO Master Proposal.dotm
7. ~$mote Service Plan-2020 v1.docx
8. Service report technical notes - ver.3.docx
9. Service report technical notes.doc
10. gotteaux PSR 2019 05 10.doc
11. Nalco Report PepsiCo Service Water Fayetteville Septemeber 2018.xlsx
12. Volkswagen - Media Center - Chilled Water System 06.11.2014.docx
13. NALCO Master Proposal.dotm
14. Remote Service Plan-2020 v1.docx

C. Search Results

The results from each of these searches are detailed below.

1. **Search No. 1 Results**: After searching for the file names of the documents identified in Search No. 1, *supra* Section III.B.1, I received no results. Therefore,

none of the file names identified in Search No. 1 exist within these custodians' emails, attachments, or OneDrive accounts.

2. **Search No. 2 Results**: After searching for the key words identified in Search No. 2, *supra* Section III.B.2, I received 14 results. I reviewed each of the results and determined that none of the resulting documents appear to contain Ecolab confidential information. For demonstration, I am including several examples of non-Ecolab documents that hit on Nalco or Ecolab. Document 1: a ChemTreat document dated January 23, 2021 (which I understand was about 6 months before Ridley left Ecolab),[21] that references Nalco in the context of identifying Nalco as the current provider being replaced by the customer with ChemTreat. Document 2: a ChemTreat-branded PowerPoint documenting technology updates, one slide of which includes a feature comparison between ChemTreat and Ecolab. This presentation shows a creation date of July 27, 2010, and the last time any modification occurred was on August 8, 2014. Documents 3 & 4 were ChemTreat-branded presentations that were related to an event that occurred in New Orleans in 2017. My review of the rest of these documents resulted in either the same type of documents clearly originating with ChemTreat, or Mr. Ridley's personal documents (such as a personal bank account statement that had the word Ecolab at the top of the statement, and a personal resume listing his employment with Nalco Water). Based on my investigation, I concluded that none of these documents had indicia suggesting they were Ecolab's documents.

[21] Ecolab's March 3, 2022 Complaint, ¶ 1 (Doc. 1).

3. **Search No. 3 Results**: After searching for the e-mail addresses identified in Search No. 3, *supra* Section III.B.3, I received 81 results. I reviewed each of the results and determined that only one of the resulting documents bears any indicia that it is an Ecolab document that may contain Ecolab confidential information. This result was an attachment to an email contained in Mr. Ridley's ChemTreat-issued email account. Neither the attachment nor the email bearing this file name exist in any other of the custodians' email accounts or OneDrive folders, or in Mr. Ridley's OneDrive folder. The attachment to this email bears a "Nalco" logo at the top right-hand side of the page and the file is entitled "AEDC proposal for purchasing – HVAC Cooling Towers – October 2015.doc". The attached document is not labeled confidential. The email is an email from Mr. Ridley's personal email account, aridley75@hotmail.com, to his ChemTreat-issued email account, titled "AEDC Proposal." The email contains no body text. This document has been produced to Ecolab in this litigation.[22]

4. **Search No. 4 Results**: After searching for the file name identified in Search No. 4, *supra* Section III.B.4, I received one result. That document is an email with an attachment and is the same email and attachment that resulted from Search No. 3 above.

5. **Search No. 5 Results**: After searching for the file name identified in Search No. 5, *supra* Section III.B.5, I received no results. Therefore, there is no document

[22] CHEMR-000001631; CHEMR-000001632. I understand Ecolab has stated in this litigation that this document is "not a trade secret individually." Ecolab's January 27, 2023 Supplemental Responses & Objections to ChemTreat's Interrogatories, at page 4.

bearing the file name identified in Search No. 5 within the OneDrive accounts accessible to the aforementioned custodians.

6. **Search No. 6 Results**: After searching for the file names of the documents identified in Search No. 6, *supra* Section III.B.6, I received no results containing those file names. Therefore, none of the file names identified in Search No. 6 exist within these custodians' emails, attachments, or OneDrive accounts.

D. Search of ChemTreat Shared Network Folders and Files

ChemTreat has certain shared network folders that are distinct from SharePoint and OneDrive.[23] I directed ChemTreat IT personnel to conduct searches across all shared network folders and files.[24] Based on my conversation with ChemTreat IT personnel, these shared network folders and files are only accessible from one of three physical ChemTreat office locations or via the VPN function, and even then, they are only accessible if access is requested and granted. There is no evidence or record that Mr. Ridley had read or write access to any of ChemTreat's shared network folders and files. Nevertheless, I directed a search of the shared network folders and files.

Specifically, I instructed ChemTreat IT personnel to search for the file names identified in Search Nos. 1, 4, and 6 across all files on ChemTreat's shared networks. I instructed ChemTreat IT personnel not to limit this search to folders or locations to which Mr. Ridley had access, but instead to include all user locations (rather than just Mr. Ridley and the custodians identified above). Because it was not limited to Mr. Ridley or the identified custodians, but rather was run across ChemTreat's entire system, this search for the 15 file names identified in Search Nos. 1, 4,

[23] Similar to OneDrive, SharePoint is a cloud-based document storage platform.

[24] I did not collect all files in ChemTreat's shared network folders because collecting these files—which cover many gigabytes and potentially terabytes of data—would be time consuming and costly, with a low likelihood of resulting in discovery of data relevant to my forensic investigation.

and 6, which ChemTreat IT personnel conducted using TreeSize Version 5.2.3, took multiple days to run to completion. This search returned no results, meaning that none of the file names from Search Nos. 1, 4, and 6 exist within ChemTreat's shared network folders or files.

E. Conclusions Based on Early 2022 Investigation

Based on my investigation in early 2022, involving the searches discussed above, and the results from those searches, I concluded that—based on the information that had been provided by Ecolab as of the filing of their March 3, 2022 complaint[25]—there was no evidence to suggest that Mr. Ridley had stored Ecolab's confidential documents on ChemTreat's Systems or that he distributed Ecolab's confidential documents using ChemTreat's Systems. As to the sole non-confidential Ecolab document identified above, I did not locate that document in any of the custodial data I searched as part of Search Nos. 4 and 5, other than Mr. Ridley's ChemTreat email account.

IV. Further Investigation in 2023

Ecolab's March 3, 2022 complaint discussed Ecolab's investigation of their electronic data and systems, including detailing the information they learned through that investigation (such as specific times and dates when Mr. Ridley allegedly downloaded specific documents or files from his Ecolab OneDrive account) that led them to conclude that Mr. Ridley had misappropriated Ecolab documents. At the time of my investigation in early 2022, however, Ecolab had not provided ChemTreat with any written report or log regarding or reflecting the information detailed in their complaint. In December 2022, Ecolab produced to ChemTreat a data loss prevention report (also known as a "DLP Report") that they represented was created using software commercially available from Digital Guardian. Using the 11,713 de-duplicated file names from that Report, I

[25] Ecolab did not provide any additional information between the filing of their March 3, 2022 complaint and the time I concluded my early 2022 investigation.

searched an even broader set of custodians, data, and temporal ranges than I had searched in early 2022 to investigate whether those files existed on ChemTreat's Systems. For clarity, as with all of the searches described in my report, these searches were run across the file names of the collected documents, the content of the collected documents (when available), and the relevant metadata fields (as identified in the ESI protocol entered by the Court)[26] for the collected documents.

A. The "DLP Report"

On December 19, 2022, Ecolab provided to ChemTreat a "DLP Report," which is a report Ecolab states was generated using Ecolab's Digital Guardian software.[27] Ecolab represented that the DLP Report was generated on July 23, 2021, using a 60-day range or "lookback" period.[28] Ecolab contends that the "Destination File Name" column of the DLP Report shows a file listing of all of the documents they allege Mr. Ridley misappropriated.[29] The DLP Report does not contain any of the actual, underlying documents whose file names are recorded in the DLP Report, nor does it include the MD5 hash values for those documents.

MD5 hash values are unique alphanumeric identifiers assigned to documents that allow a viewer to determine whether one document is identical to another document; they function as a document's "fingerprint." Without these MD5 hash values (and absent the underlying documents from the DLP Report), the only means of assessing whether the documents from the DLP Report are identical to other documents is to compare file names, although a more comprehensive search

[26] December 14, 2022 Agreed Order Regarding Protocol for Production of Hard Copy Documents and Electronically Stored Information (Doc. 91).

[27] Ex. E, December 19, 2022 1:18 p.m. email from D. Walton to J. Lund and T. Homesley.

[28] Ex. E, December 19, 2022 1:18 p.m. email from D. Walton to J. Lund and T. Homesley.

[29] *See* Plaintiffs' January 26, 2023 Notice of Completion of Post-Motion Meet and Confer, at 2 (Doc. 119); ChemTreat's February 13, 2023 ESI Report, at 2 (Doc. 143).

would involve a search for MD5 hash values. I have received the DLP Report and used it for the search discussed below.

B. Search Parameters

Because Ecolab alleges that Mr. Ridley stored, used, and potentially distributed the files listed on the DLP Report, I searched for the file names associated with all of those files across various potentially relevant custodians and repositories. The only means of identifying potentially overlapping documents is via a file name search (including by searching for the file names across the content of documents and relevant metadata), although this methodology is sure to return false "hits." I used the "Destination File Name" column of the DLP Report to determine which file names to search for. Many of the file names are duplicates, meaning that they are identical file names (for example, the file name "image1.jpg" appears on the DLP Report multiple times). After removing duplicates (which need not be searched twice), the total number of file names to be searched was 11,713. Attached as Exhibit F is a list of the file names I searched for (de-duplicated).

Using the file names listed on the DLP Report provided to ChemTreat by Ecolab, I conducted a search for all of the de-duplicated file names listed on the DLP Report across a broader set of data than I searched as part of my early 2022 investigations. Specifically, I searched for 11,713 unique file names across the emails and OneDrive data available for 14 custodians. These custodians were the same custodians used for purposes of my early 2022 investigation, but also included the addition of Tyler Bates, who had been identified by Ecolab in the intervening months as someone with whom Mr. Ridley may have shared Ecolab's confidential information.[30] Based

[30] Ecolab's June 10, 2022 Second Amended Complaint, ¶¶ 192-94 (Doc. 42). Mr. Bates's OneDrive documents were collected after Ecolab identified him in its Second Amended Complaint.

on that search, I concluded that none of the files listed on the DLP Report had been distributed or stored on ChemTreat's Systems.

Notably, many of the file names I searched for caused a high hit count based on the file name being "generic." Generic file names appear quite often with images. For example, the word "image" (e.g., image1.jpg, image2.jpeg, etc.) is contained within file names on the DLP Report. This is a common type of generic file name. I expected that these generic file names would return "hits" as a result of the search, even though they may not contain Ecolab's confidential information—or have anything to do with Ecolab at all. Files that generally have these "generic" file names include images associated with signature blocks, which are often split into separate documents and often reflect corporate logos or phrases. Based on my review of these generic "hits," it is clear that the generic "hits" are not related to Ecolab at all. For example, many of these generic "hits" are personal photographs, or images that bear ChemTreat's logo or information.

As noted, I searched for the search terms identified in Exhibit F across the potentially relevant custodians, devices, and repositories. For email data, an overbroad temporal range was used to ensure all potentially relevant emails from prior to Mr. Ridley's recruitment until after his termination.[31] Below are the repositories and custodians I searched:

- Mr. Ridley's ChemTreat emails.
- All documents accessible to Mr. Ridley via OneDrive.
- File names of all documents accessible to Mr. Ridley via SharePoint.[32]

[31] CHEMR-000000147 (showing Mr. Ridley's contact with ChemTreat on August 17, 2020); March 21, 2022 Ltr. from V. Mirmira to D. Walton (Doc. 52-1) (showing Mr. Ridley was terminated on March 18, 2022).

[32] For this search, I requested a file directory that would show the file names of the files accessible to Mr. Ridley via SharePoint, which was all that was necessary to determine if any of the at-issue file names existed in SharePoint folders accessible to Mr. Ridley.

- Mr. Ridley's ChemTreat-provided cell phone.[33]
- Emails of the following custodians for the temporal period July 1, 2020 through April 1, 2022: Tyler Bates, John Alcorn, Clay (Richard) Cissell, Albert DeNunzio, David Ellis, Larry Harmon, Matthew Hofer, Michael (Todd) Kraft, Steven Leavell, David Pearson, James (Jim) Shealy, George Sloan, and John Spalding.
- All documents accessible to the following custodians via OneDrive as of March 16, 2022: Tyler Bates, John Alcorn, Richard (Clay) Cissell, Albert DeNunzio, Larry Harmon, Matthew Hofer, Michael (Todd) Kraft, Steven Leavell, David Pearson, James (Jim) Shealy, George Sloan, and John Spalding.
- Mr. Ridley's Lexar USB device issued to him by ChemTreat.
- The complete CrowdStrike log.[34]

C. Results

Below is a chart that lists the results of my search. The vast majority of "hits" were on generic documents. I reviewed each "hit" and, as shown below, did not locate any documents that appeared to contain Ecolab's confidential information. Based on my review of these generic "hits," it is clear that the generic "hits" are not related to Ecolab at all. For example, many of these generic "hits" are personal photographs, or images that bear ChemTreat's logo or information.

[33] I forensically imaged Mr. Ridley's ChemTreat-provided cell phone when it was sent to me in early 2022. I searched the locations of Mr. Ridley's ChemTreat-provided cell phone where documents are routinely housed.

[34] Because I was unable to view the documents corresponding to file names in the CrowdStrike log, I relied on the file names to ascertain whether the documents appeared to contain Ecolab confidential information. These generic file names did not appear to correspond to any Ecolab confidential information. *See* Ex. H (listing the DLP Report file names that matched file names in the CrowdStrike log).

Repository	Total Hits	Generic Hits	Non-Generic Hits	Ecolab Documents
Mr. Ridley's ChemTreat Emails	171	170	1	1 (AEDC proposal for purchasing – HVAC Cooling Towers – October 2015.doc[35])
Mr. Ridley's OneDrive Folders	599	599	0	0
Mr. Ridley's SharePoint Folders	1	1	0	0
Mr. Ridley's ChemTreat-Provided Cell Phone	0	0	0	0
Other Custodians' Emails[36]	671	671	0	0
Other Custodians' OneDrive Folders[37]	1	1	0	0
Mr. Ridley's Second ChemTreat-Issued Laptop	277	277	0	0
Mr. Ridley's Lexar USB (Serial No. 56261F6B34AF1760)	3	3	0	0
CrowdStrike Log	25	25	1	1 (AEDC proposal for purchasing – HVAC Cooling Towers – October 2015.doc[38])

As shown above, there was only one non-generic file name corresponding to a file name in the DLP Report across all sources searched. That non-generic file name corresponded to the sole Ecolab document I had previously identified as part of my original investigation in early 2022.[39]

[35] CHEMR-000001632.

[36] *See* custodians referenced *supra*, Section IV.B.

[37] *See* custodians referenced *supra*, Section IV.B.

[38] CHEMR-000001632.

[39] CHEMR-000001632.

Finally, as an additional confirmatory measure, I searched across Mr. Ridley's outgoing emails to determine whether he sent any other ChemTreat employees any electronic links to files on his OneDrive or another networked location on ChemTreat's Systems, or links to allow sharing of his OneDrive files. I did not locate any such links or distribution of files via linked systems, indicating that Mr. Ridley did not provide access to his OneDrive folders to any other ChemTreat employees during his employment at ChemTreat.

D. Mr. Ridley's Ecolab-Issued Laptop and "LaCie Drive"

Because Ecolab has not produced Mr. Ridley's Ecolab-issued laptop or a forensic image of that laptop in this litigation, I was unable to compare documents or data from Mr. Ridley's Ecolab issued laptop with documents or data on ChemTreat's Systems. Based on the discovery material I have reviewed, I understand that Ecolab has stated in this litigation that it "removed all data" from Mr. Ridley's Ecolab-issued laptop when the laptop was returned to Ecolab by Mr. Ridley in July 2021 and that Ecolab "restored [the laptop] to factory settings."[40]

Ecolab also has not produced the "LaCie Drive," serial number def10dce9db4 (as reflected on the DLP Report), which is an external hard drive that the DLP Report reflects many of the allegedly misappropriated files may have been transferred to. Based on Ecolab's complaint, I understand it is unable to confirm whether the "mobile drive" that Mr. Ridley returned to Ecolab in July 2022 was the "LaCie Drive" identified in the DLP Report.[41] Based on the discovery material I have reviewed, I understand that Ecolab has stated that it cannot locate and may have "destroyed" the "mobile drive" that was returned to them and so does not know whether that "mobile drive" is the same external hard drive as the "LaCie Drive" referenced in the DLP

[40] Ecolab's January 27, 2023 Supplemental Responses & Objections to ChemTreat's Interrogatories, at page 13.

[41] Ecolab's June 10, 2022 Second Amended Complaint, ¶ 151 (Doc. 42).

Report.[42] Based on the discovery material I have reviewed, I further understand that Mr. Ridley has stated under oath that he returned the "LaCie Drive" to Ecolab.[43]

To determine whether Mr. Ridley accessed documents on the "LaCie Drive" using his first ChemTreat-issued laptop, I searched in the CrowdStrike log for the serial number associated with the "LaCie Drive" in the DLP report provided by Ecolab. In order to conduct this search, I received a complete copy of the CrowdStrike log.[44] Neither the serial number (def10dce9db4) nor the term "LaCie" appeared in the CrowdStrike log, meaning that Mr. Ridley did not access any files from the "LaCie Drive" on his first ChemTreat-issued laptop.

E. Reasonableness of the Investigation I Conducted

Based on more than 20 years of experience as a digital forensics examiner, the search I conducted was reasonable and sufficient to identify and locate any files on ChemTreat's Systems that may contain the file names corresponding to the documents Ecolab alleges Mr. Ridley misappropriated. As noted above, while the searches I conducted during my early 2022 investigation and my subsequent investigation returned some "hits," upon review, it was clear that the "hits" corresponded to documents that do not contain Ecolab's confidential information (with the exception of the sole Ecolab document identified during my early 2022 investigation, as discussed above). I briefly describe here why the parameters of the investigation I conducted were both reasonable and appropriate under the circumstances.

Search Terms: As discussed above, during my investigation in early 2022, I searched for file names based on the allegations in Ecolab's March 3, 2022 complaint, and performed additional

[42] Ecolab's January 27, 2023 Supplemental Responses & Objections to ChemTreat's Interrogatories, at page 14.
[43] Ridley's July 20, 2022 Responses & Objections to Ecolab's Interrogatories, at pages 19-20.
[44] CHEMR-000002195.

searches on Mr. Ridley's OneDrive using the broad terms "Nalco" and "Ecolab". After Ecolab provided the DLP report to ChemTreat, I used the file names from the "Destination File Name" field of the DLP Report as search terms when conducting my investigation of the file names identified on the DLP report. Also as described above, given that Ecolab has not produced the underlying documents corresponding to the file names in the DLP Report and has not provided the MD5 hash values associated with those file names, searching for these file names was the only comprehensive means of searching for Ecolab's allegedly misappropriated confidential information. I understand that Ecolab has taken the position that a comprehensive investigation requires ChemTreat to search for the file names "identified on the Digital Guardian data loss prevention report,"[45] which is what I have done.

Temporal Range: The temporal range applicable to the investigation I conducted was reasonable and comprehensive. The beginning of the temporal range extended more than a month before what I understand was ChemTreat's earliest discussions with Mr. Ridley regarding his potential employment.[46] The end of the temporal range extended almost two weeks beyond Mr. Ridley's departure from ChemTreat.[47] And, as for the OneDrive documents, the investigation I conducted was of the various custodians' OneDrive documents as they existed contemporaneously with (but immediately prior to) Mr. Ridley's termination by ChemTreat, meaning the investigation would reveal any relevant OneDrive documents as they existed immediately prior to Mr. Ridley being informed of his termination.

[45] Ecolab's January 26, 2023 Notice of Completion of Post-Motion Meet and Confer Process, at 2 (Doc. 119).

[46] CHEMR-000000147 (showing Mr. Ridley's contact with ChemTreat on August 17, 2020).

[47] ChemTreat's July 22, 2022 Responses & Objections to Plaintiffs' Interrogatories, at page 9.

Custodians: Based on the assumptions provided to me by ChemTreat's counsel, the custodians whose data I searched included the business people at ChemTreat with whom Mr. Ridley may have interacted, including those within Mr. Ridley's line of authority. These individuals include Mr. Ridley himself, Mr. Ridley's immediate supervisor, the supervisor to Mr. Ridley's supervisor, Mr. Ridley's predecessor, the executive at the head of ChemTreat's North American field sales organization, and a number of ChemTreat employees who may have interacted with Mr. Ridley.

Repositories: The repositories I investigated include each of the repositories that a digital forensics examiner seeking to confirm the presence or absence of Ecolab's confidential information on ChemTreat's system would investigate to determine whether Mr. Ridley had distributed or stored such information. My investigation involved a broad range of repositories, including cloud accounts (such as OneDrive and, for Mr. Ridley, SharePoint); email searches that would show email distributions of documents or links to documents, as well as communications about the at-issue file names; and even searches of devices issued to Mr. Ridley during his tenure at ChemTreat. Despite the breadth of my investigation, my investigation did not reveal any evidence supporting Ecolab's allegations that Mr. Ridley stored or distributed Ecolab's confidential information on ChemTreat's systems. For example, while I located a single Ecolab document in Mr. Ridley's email account (CHEMR-000001632), which does not bear any confidentiality designation and which I understand Ecolab has indicated is not a standalone trade secret,[48] I did not see any evidence of Mr. Ridley transmitting this document to anyone else. I also

[48] Ecolab's January 27, 2023 Supplemental Responses & Objections to ChemTreat's Interrogatories, at page 4.

did not see any evidence of Mr. Ridley emailing any other Ecolab documents (whether confidential or otherwise) to himself or to any other ChemTreat employees.

As noted above, ChemTreat has certain shared network folders beyond OneDrive and SharePoint. Based on my conversation with ChemTreat IT personnel, these shared network folders and files are only accessible from one of three physical ChemTreat office locations or via the VPN function, and then only accessible if access is requested and granted. There is no evidence or record that Mr. Ridley had read or write access to any of ChemTreat's shared network folders and files. While I searched these shared network folders as part of my initial investigation for a relatively small number of file names that had been identified as potentially relevant file names at that time, I subsequently determined that no further search was necessary as there was no evidence Mr. Ridley had access to these folders. Moreover, it would not be relevant or economical to search these shared network folders for the 11,713 file names identified in Exhibit F. As discussed above, when I directed ChemTreat to run searches for the 15 file names identified in Search Nos. 1, 4, and 6 as part of my investigation in early 2022, the search for just those 15 file names took multiple days to run to completion.

Searches Are Burdensome: Here, I note that searching for documents and file names is a time consuming and burdensome endeavor. Therefore, the ability to search for documents should not be limitless. Searches for documents across complex digital systems should be confined by specific parameters. The investigation I conducted balanced these burden concerns against the need to search the repositories and custodians potentially likely to contain relevant information.

F. Reliability of the CrowdStrike Log and Validation Testing

Ecolab has asserted in this litigation that, during his employment by ChemTreat, Mr. Ridley accessed or used documents he allegedly misappropriated from Ecolab.[49] In order to assess this allegation, I reviewed and searched the CrowdStrike log produced in this litigation, which was generated in March 2022 by Adam Fisher, a Cybersecurity Engineer in ChemTreat's Water Quality Group. As discussed above, *see supra*, Section III.A.1.d, the CrowdStrike log would show Mr. Ridley's interactions with any documents that were accessed from any external USB device, using his first ChemTreat-issued laptop, as well as any documents that were saved on that laptop after being opened from an external device. As discussed above, that search revealed Mr. Ridley's interaction with a narrow set of documents that could potentially belong to Ecolab.

Although the underlying documents are not available, such that I cannot assess whether they actually contain Ecolab's confidential information, given that the CrowdStrike log created after the reformatting of Mr. Ridley's first ChemTreat issued laptop reflects Mr. Ridley's limited interactions with documents containing the phrase "Nalco Water Files" in the file path name, I wanted to validate that a CrowdStrike log created after the reformatting of a laptop is capable of capturing all of the user's interactions with documents from external devices predating that reformatting. To validate the interactions reflected on the CrowdStrike log for Mr. Ridley's first ChemTreat-issued laptop, I conducted the validation procedures identified below. Based on those validation procedures, I was able to confirm that CrowdStrike logs all interactions a subject laptop has with any documents accessed from an external device, and retains that information even after the subject laptop is reformatted. Accordingly, I conclude that the limited interactions between Mr. Ridley's first ChemTreat-issued laptop and documents accessed from an external USB device

[49] Ecolab's June 10, 2022 Second Amended Complaint, ¶ 108 (Doc. 42).

that are reflected on the CrowdStrike log produced by ChemTreat in this litigation accurately reflect the full scope of interactions that Mr. Ridley had with documents that were accessed from any external USB device using his first ChemTreat-issued laptop, or that were contemporaneously saved to the laptop after being opened from the connected USB device.

1. Temporal Ranges of the CrowdStrike Log

The CrowdStrike log shows activity on Mr. Ridley's first ChemTreat-issued laptop covering the period from July 9, 2021, through February 28, 2022. To confirm that the log was properly created and captured all of Mr. Ridley's relevant activity for the time period of his possession of the laptop, I validated this time period by considering various factual circumstances based on the documents and information available to me.

a. Beginning Date of the CrowdStrike Log

I understand that Mr. Ridley resigned from Ecolab on July 1, 2021.[50] The contemporaneous documents I reviewed reflect that, due to supply chain issues, Mr. Ridley did not receive his first ChemTreat-issued laptop until July 12, 2022 at the earliest.[51] The first activity in the CrowdStrike log associated with Mr. Ridley's user profile occurred on July 12, 2021. July 13, 2021 is the first date on which Mr. Ridley sent emails from his ChemTreat email account.[52] Based on this information, I conclude that July 12, 2021 is the first date that Mr. Ridley accessed or used his ChemTreat-issued laptop. The CrowdStrike log shows activity as early as July 9, 2021, but that activity is not associated with Mr. Ridley's user profile. The presence of that activity on the CrowdStrike log is consistent with the log capturing activity associated with ChemTreat's IT personnel setting up the laptop before it was sent to Mr. Ridley. Based on my experience, it would

[50] Ecolab's June 10, 2022 Second Amended Complaint, ¶ 1 (Doc. 42).
[51] CHEMR-000001543; CHEMR-000001530.
[52] *E.g.*, Ex. C, July 13, 2021 email from A. Ridley to S. Freed.

be unusual not to have such activity reflected on a log such as the CrowdStrike log, as businesses with dedicated IT personnel typically have a standard process for setting up laptops before deployment to employees, including installing standard software and security measures.

b. End Date of the CrowdStrike Log

The CrowdStrike log for Mr. Ridley's first ChemTreat-issued laptop reflects no activity associated with Mr. Ridley's user profile after February 28, 2022. Based on my review of the contemporaneous documents and discovery material I was provided, this end date is consistent with Mr. Ridley returning his first ChemTreat-issued laptop to ChemTreat for preservation purposes at the end of February 2022.[53] Mr. Ridley was provided a second ChemTreat-issued laptop to replace his first ChemTreat-issued laptop when he was instructed to return that first ChemTreat-issued laptop. Mr. Ridley's second ChemTreat-issued laptop was collected and preserved upon his termination. As discussed above, I forensically imaged and forensically analyzed Mr. Ridley's second ChemTreat-issued laptop.

2. Information Contained in the CrowdStrike Log

The CrowdStrike log tracking Mr. Ridley's interactions with external USB devices contains the following "headers" reflecting information collected and logged by CrowdStrike:

<field>time</field>
<field>name</field>
<field>VolumeDriveLetter</field>
<field>VolumeName</field>
<field>DeviceManufacturer</field>
<field>DeviceProduct</field>
<field>DeviceSerialNumber</field>
<field>DeviceInstanceID</field>
<field>TargetFileName</field>

[53] *See* CHEMR-000001840.

Each of these "headers" or fields provide information about the name of a file accessed from an external USB device, the date and time it was accessed, and the USB device from which it was accessed. These fields are relevant because these fields capture information a forensic examiner like myself would rely on regarding interactions with external USB devices, and files on those devices. There is no other material field, that is not included, that prevents me from reaching the conclusions I have reached regarding my CrowdStrike log analysis. Based on my review of the CrowdStrike log generated by ChemTreat, it is apparent that Mr. Fisher used a query that captured the broadest possible set of information regarding Mr. Ridley's user activity on his first ChemTreat-issued laptop.

The CrowdStrike log contains 12,354,453 lines of XML data. This amount of data can be lost when converted to an Excel format, so the CrowdStrike log was exported to an XML format to ensure all data was captured. [54]

3. Validation and Testing Procedure

I used the following validation and testing procedure to confirm the accuracy, reliability, and completeness of the CrowdStrike log of Mr. Ridley's first ChemTreat-issued laptop. First, I requested that ChemTreat provide me with a laptop that used the same OS (operating system) as Mr. Ridley's first ChemTreat-issued laptop, which I understand was Windows 10. Second, I requested that ChemTreat provide me with the same access parameters available to Mr. Ridley. Third, I requested that ChemTreat confirm whether the CrowdStrike platform used by them during the time period of my validation testing (February 2023) was materially similar to the CrowdStrike platform used by ChemTreat at the time ChemTreat's IT personnel generated the CrowdStrike log

[54] Excel specifications and limits, *available at* https://support.microsoft.com/en-us/office/excel-specifications-and-limits-1672b34d-7043-467e-8e27-269d656771c3.

of Mr. Ridley's first ChemTreat-issued laptop (March 2022). I determined that ChemTreat's CrowdStrike configurations have remained materially constant for the last two years, such that there are no material differences in the information collected or logged by CrowdStrike in March 2022 and February 2023. While ChemTreat has deployed regular "sensor updates," these "sensor updates" would not materially impact the activities captured by CrowdStrike.

After determining that these variables were consistent, I conducted a testing procedure on the test laptop I requested from ChemTreat. Specifically, I conducted various experiments with the test laptop by (1) plugging in an external USB and opening files from that USB using Microsoft Office and PDF applications; (2) plugging in an external USB and opening files from that USB using Windows Explorer; and (3) plugging in an external USB, opening and then saving files from that USB to the test laptop's hard drive.

Following these experiments, I sent the laptop back to ChemTreat with the instruction that their IT personnel should reformat the laptop in the same manner that they had reformatted Mr. Ridley's first ChemTreat-issued laptop. I then requested that Mr. Fisher generate a CrowdStrike log for this validation laptop that contained the same "headers" contained in the original CrowdStrike log he generated for Mr. Ridley's first ChemTreat-issued laptop. Next, I analyzed the CrowdStrike log generated for the validation laptop to determine whether it reflected the various electronic activities described above.[55]

[55] *See* Ex. G, Validation CrowdStrike Log. The Validation CrowdStrike Log was exportable as a csv file because it contained just 35,043 rows of data and thus was orders of magnitude smaller than the CrowdStrike log produced in this litigation. The CrowdStrike log produced in this litigation had to be exported as an XML file to capture all relevant data because it covered a broader time frame, more activity, and contained over 12 million lines of data.

4. Results

Based on this validation and testing procedure, I confirmed that the CrowdStrike log generated for the validation laptop accurately and reliably captured all of the activity described above, despite the intervening reformatting of that validation laptop. Additionally, the CrowdStrike log generated for the validation laptop accurately captured the serial number of the USB device used for validation purposes. This is exactly how CrowdStrike is supposed to function: It does not depend on the continued existence of a physical device, but acts as an endpoint protection and antivirus software that detects and logs the presence of external devices and access to external files in real time. CrowdStrike perceives those files as a potential threat, even if they are benign, which is why it logs each and every interaction with a file that is accessed from an external device.

5. Conclusion Regarding Validity and Reliability of the CrowdStrike Log

Having conducted this validation and testing procedure, I can state to a reasonable degree of certainty, based on my expertise as a digital forensics examiner, that the CrowdStrike log produced to Ecolab in this litigation accurately and reliably reflects the file names of any files from any external devices (such as a USB or external hard drive) that Mr. Ridley interacted with using his first ChemTreat-issued laptop.

G. Conclusion Arising from Further Investigation in 2023

Consistent with the findings of my investigation in early 2022, I did not locate any evidence that Mr. Ridley distributed or stored documents containing Ecolab's confidential information on or through ChemTreat's Systems.

V. Conclusions

Based on the foregoing and relying upon my more than 20 years of experience and expertise as a certified digital forensics examiner, I conclude, based upon the analysis of all evidence available to me, that there is no evidence that Mr. Ridley stored Ecolab's confidential information on ChemTreat's Systems. I further conclude that there is no evidence that Mr. Ridley distributed Ecolab's confidential information to other ChemTreat employees using ChemTreat's Systems. Finally, I conclude that Mr. Ridley may have interacted with a very limited set of documents that bear file names indicating that they may have originated with Ecolab, although he did not upload those documents to ChemTreat's Systems or use ChemTreat's Systems to distribute them. However, because I do not have access to those documents, either from ChemTreat or from Ecolab, I cannot review them to determine whether they contain indicia suggesting they actually belong to Ecolab or contain Ecolab's confidential information.

Signed: 
James D. Vaughn

Dated: February 21, 2023